(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 September 2005 (01.09.2005)

PCT

(10) International Publication Number
WO 2005/081085 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2005/004877

(22) International Filing Date: 11 February 2005 (11.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/544,809 13 February 2004 (13.02.2004) US
60/613,059 24 September 2004 (24.09.2004) US

(71) Applicant *(for all designated States except US)*: **THE REGENTS OF THE UNIVERSITY OF CALIFORNIA** [US/US]; 10920 Wilshire Boulevard, Suite 1200, Los Angeles, CA 90024-1406 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VERBAUWHEDE, Ingrid** [US/US]; 1123 23rd Street #C, Santa Monica, CA 90403 (US). **TIRI, Kris, J.V.** [BE/BE]; De Hutten 16, B-3600 Genk (BE).

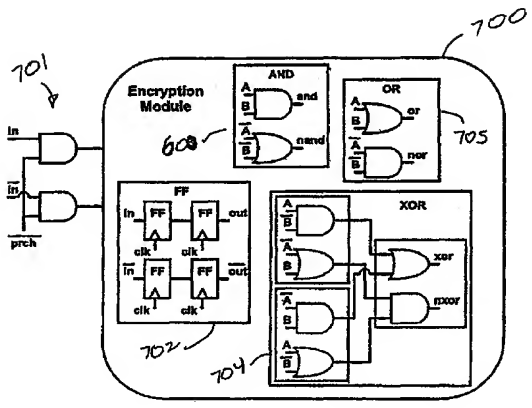
(74) Agent: **ALTMAN, Daniel, E.**; KNOBBE, MARTENS, OLSON AND BEAR, LLP, 2040 Main Street, Fourteenth Floor, Irvine, CA 92614 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,

[Continued on next page]

(54) Title: LOGIC SYSTEM FOR DPA AND/OR SIDE CHANNEL ATTACK RESISTANCE



(57) Abstract: DPA-resistant logic circuits and routing are described. An architecture and methodology are suitable for integration in a common automated EDA design tool flow. The architecture and design methodology can be used in logic circuits, gate arrays, FPGAs, cryptographic processors, etc.In one embodiment, the implementation details of how to create a secure encryption module can be hidden from the designer. The designer is thus, able to write the code for the design of DPA-resistant logic circuits using the same design techniques used for conventional logic circuits. Contrary to other complicated DPA-blocking techniques, the designer does not need specialized knowledge and understanding of the methodology. In one embodiment, the automated design flow generates a secure design from a Verilog or VHDL netlist. The resulting encryption module has a relatively constant power consumption that does not depend on the input signals and is thus relatively independent of which logic operations are performed. In one embodiment, the present design methodology uses existing resources and as a result can be readily applied. In one embodiment, the architecture and design methodology blocks DPA at the logic level, freeing the designer to concentrate on preventing other side channels at a different level of abstraction (e.g., conditional branching with unequal lengths, etc.)

WO 2005/081085 A2

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.